TABLE OF CONTENTS

1 INTRODUCTION

This document describes some of the current service standards provided by the Department of Technology Services (DTS), also known as the State Data Center. The documents included within describe the service standards that may be affected by the implementation of the California Department of Corrections and Rehabilitation (CDCR) Business Information System project (BIS) Project. However, the State Data Center Statement of Work (DC SOW) for BIS will require some changes to these current service standards. These changes will occur as part of the BIS Project.

BIS Project is an Enterprise Resource Planning (ERP) Solution which will streamline CDCR's administrative business processes to ensure efficient, cost-effective fulfillment of the Department's mission The State Data Center will provide the application hosting for the BIS Project.

The documents included are in draft format and are periodically updated. However, these are the most current versions. In addition, data included in each section is specific to that particular service standard.

(NOTE: This document is for informational purposes only and does not constitute a real or implied contractual agreement between the BIS Project and the State Data Center. As mentioned above, there are deviations between the State Data Center BIS SOW and these standard service offerings. Close attention should be given to both documents to determine differences when costing the service for the BIS Project.)

2 STATE DATA CENTER MIDRANGE SYSTEMS APPLICATION HOSTING

2.1 Explanation of the Service Standard

2.1.1 Statement of Service

Broadly available software applications are a vital component of many businesses. Ensuring that these applications are hosted in a reliable, secure, and technologically up-to-date environment is, for many organizations, difficult, expensive, and a drain on technical support staff. The State Data Center offers extensive, secure processing, monitors computing availability and performance, and provides backup and recovery capabilities.

The State Data Center provides software application hosting on midrange servers running Windows 2000/2003 or UNIX (AIX, Solaris) operating systems (OS). The application servers are located in a secure, environmentally controlled, raised floor computer room. The State Data Center provides a full power system redundancy and a fire suppression system.

2.1.2 Service Standard Highlights

The State Data Center Midrange Application Hosting service standard includes:

- Hardware procurement, installation, and maintenance for servers

- Software procurement, installation, and maintenance for servers (operating system, system utilities, database, and web software)
- Performance monitoring of hardware, software, and databases
- Network connectivity
- Environmentally controlled secure facility
- Reliable power with full uninterruptible power supply (UPS) and generator backup
- Halon fire suppression system
- System backup and recovery
- Security systems including virus protection, data encryption, and intrusion detection

2.1.3 System Response Time

Both the Customer and the State Data Center monitor the health of the system. Various factors determine the user's wait-time when executing a command from their keyboard/mouse. These factors include: the configuration of individual customer networks, the speed of the desktop processor, the amount of available RAM on a desktop, and the type of software package executed. These factors can vary from one desktop to the next so system response times will also vary. Additional functionality and configuration of customer LANs can also impact system response time.

The State Data Center maintains system benchmark and service delivery as per industry standards but due to aforementioned variables, cannot make any guarantees for end-to-end system response time. However, internal response time measurements can be negotiated and measured on a case by case basis with the customer. Service Level Agreements are negotiated at customer service startup time.

2.1.4 System Monitoring

Operational considerations included in the State Data Center system monitoring are:

- Daily check of the backup logs to ensure system backups have executed properly
- On going monitoring of system availability and system performance

If any problems or issues are discovered, the State Data Center contacts the customer to coordinate the implementation of a problem solution.

2.1.5 Operations Support

The State Data Center is staffed 24 hours per day, seven days a week and provides system monitoring and availability: support for the server environment, manages tape handling, and manages customer backups.

2.1.6 Data Backup

The State Data Center performs the necessary backups of the server environments in order to guarantee both the integrity of the customer's data and to provide the ability to recover data as needed. The State Data Center retains 30 days of full system backups. Tapes are taken offsite within 24 hours.

Server backups prior to any system or application maintenance procedure may be requested at any time.

The State Data Center provides enough disk space to preserve a minimum of 31 days of full system backups. In addition, the State Data Center is responsible for monitoring system backup logs to ensure that all backups are successfully completed. If a system backup fails, the State Data Center identifies and corrects the problem to ensure the system(s) is properly backed up.

The State Data Center is responsible for managing and reporting on the following system backup activities:

- Manage backup and file rotation; tapes are scratched after 30days
- Backing up servers prior to any system maintenance procedure for which there is a potential for data loss.

2.1.7 Restore Request Process

- The requestor must obtain authorization from their department's approving authority (identified at service setup).
- Once authorization is received, the requestor contacts their department's help desk to open a help desk ticket. If no departmental help desk function exists, the requestor contacts the State Data Center Help Desk to open a ticket.
- The ticket is assigned to the appropriate Database Services Unit.
- If the requested data is onsite, data center staff restores the requested data.
- If the requested data is not onsite, the data is requested from off site storage through State Data Center Help Desk. Once the data is received and restored, the customer receives notification within 24 hours. Once the customer is satisfied with the results of the restore, the ticket will be closed.

2.1.8 Operational Recovery

The State Data Center responds to system failures within two hours during normal operating hours.

2.1.9 Disaster Recovery

For an additional cost, Disaster Recovery plans will be developed with each customer on a case by case basis.

2.1.10 Security

The State Data Center takes all necessary precautions to protect midrange systems servers from unauthorized access including modification, deletion, or disclosure of the databases, application files, and operating systems.

The State Data Center and the customer are responsible for ensuring the protection of confidential data stored and transmitted. Additionally, the State Data Center performs logging and tracking of security events should they occur. Security events are detected by intrusion detection, security sequencing, and server system and file access failures.

The customer agrees to exercise reasonable efforts to safeguard the following information:

- Specific version information of the systems' firmware, operating system, and applications in order to minimize the potential exploitation of vulnerabilities prior to release and application of service packs/fixes
- Account names/passwords
- IP addresses/system names

The State Data Center and the customer are responsible for notifying the appropriate security representative (usually the Information security Officer) of any suspected unauthorized access.

The State Data Center and the customer are responsible for maintaining hardware and software at vendor supported levels. Customers are responsible for maintaining application software at the supported levels of the system software. If customers delay in updating application software, additional support costs will be incurred.

2.2 Roles and Responsibilities

The State Data Center's experience with other midrange customers provides the expertise to help customers deploy their application solutions. The State Data Center's technical support staff sets up and configures the application server to integrate efficiently with each customer's network configuration and user population size. The State Data Center continually analyzes the hosting infrastructure to ensure operational integrity and the ability to grow as needed.

2.2.1 State Data Center Responsibilities

2.2.1.1 Provide Performance Analysis

- Track and report on resource utilization
- Provide maintenance of monitoring and data gathering tools, such as NetIQ, Compaq, Insight Manager, and HP Open View
- Notify the customer of storage capacity and/or performance issues the State Data Center discovers

2.2.1.2 Provide Server OS Support

- Perform installation, tuning, and maintenance of Operating System (OS) and related utilities
- Troubleshoot server hardware and OS
- Backup and restore the OS. This includes OS file restores or reinstalls as necessary.

2.2.1.3 Provide System Database Support

- Perform installation, tuning, maintenance and troubleshooting of database software
- Write and maintain database shutdown and startup scripts
- Provide application data backup and recovery, generally at the table level

2.2.1.4 Provide Enterprise Storage Support

- Provide installation, tuning, maintenance, and troubleshooting of storage subsystem (i.e., SAN)
- Provide installation and maintenance of enterprise storage backup solutions for enterprise storage

2.2.1.5 Provide Network Connectivity

- Establish connectivity from servers to an existing DTS/customer network
- Establish isolated connectivity and firewall protection (purchased separately as part of DTS's Network Access Service Standard)

2.2.2 Customer Responsibilities

The following are the functional areas that the customer must provide:

2.2.2.1 Server System Administration

- Provide a single point of contact to State Data Center support staff as needed.
- Develop and maintain OS interfaces.
- Provide user account administration

2.2.2.2 Application Database Support

- Provide a single point of contact to State Data Center support staff as needed
- Provide database development and support (data administrator)

2.2.2.3 Application Support

- Adhere to industry recommended security standards for application development.
- Provide development and maintenance of the application
- Provide development and maintenance of the application to all OS interfaces
- Provide configuration management for migrating objects into production

2.2.3 Joint Responsibilities (State Data Center and Customer)

Both parties are responsible for the following:

- Provide change management processes that facilitate system and application changes
- Provide user acceptance testing after a database restore

2.3 Pricing

2.3.1 Basic Service Standard Pricing

Rates are available in the DTS Rates Schedule.

2.3.2 Options

The standard build information for the DTS MidRange environment includes the following operating systems:

AIX Platform:

Hardware Platform:
PowerPC_POWER4 CPU
64-bit CPU-Type
Server hardware platform is of pSeries Logical Partitioning (LPAR)
Note: LPARs are managed with IBMs Cluster Systems Management (CSM) software.

Operating System:
AIX 5.2 within 12 months of current maintenance level
32-bit or 64-bit Kernel Type
Security updates/fixes per Patch Management Process
Note: Please refer to Security Policy Manual on our intranet: URL = http://intranet/overview/pandc/security/manual.asp

Required Component:
Cluster Systems Management Client (current version - 1.4.0.2)
Lightweight Directory Access Protocol Client (current version - 5.2.0.0)

External Storage:
All customer applications and data are contained in a SAN environment supported by the DTS Engineering Enterprise Storage Group
All backup and restoration services are also provided by DTS Engineering Enterprise Storage Group
EMC Data Manager Client (current version - 4.3)
Solutions Enabler (current version 5.4.1)
EMC Powerpath (current version 4.2.0.0)
Symmetrix (current version 5.0.0.0)

Security:
Client for Symantec Enterprise Security Manager (agentd)
Secured Shell (SSH) Client - OpenSSH (current version - 3.7.0.0)
Note: ftp, rcp, telnet are disabled and sftp, scp, and ssh are required respectively.

Performance Monitoring Tool:

NetIQ AppManager 6.0 - will be available around Dec 2005
Note: Generally not available for use by customer, however, specific data collection, monitoring, and reporting can be supplied to customer upon request.

Software:
Visual Age C++ Compiler (current version - 6.0)
JAVA Runtime (current version - 1.3.1.16)
sudo (current version - 1.6.7-p5-2)
TCP/IP daemon security wrapper (current version - 7.6.1.0)
expect (current version - 5.34-8)
lsof (current version - 4.61-3)
mkisofs (current version - 1.13-4)
tcl (current version - 8.3.3-8)
tk (current version - 8.3.3-8)

Windows Platform:

Symantec Anti-Virus 9.0
CA Unicenter Software Delivery
CA Unicenter Asset Management
HP SIM
Vertias Backup Exec 9.1
Diskeeper 8.0
HP Openview (ping for up down alerting)
Remedy Helpdesk
NetIQ AppManager (won't be implemented until August or September)

Sun Solaris:

SUN standard commands and utilities - no additional packages.

SUN standard commands and utilities, Veritas Volume manager, we capture data in a performance database and create reports using SAS.

Remedy Action Request System

Security Software:

Troubleshooting: SuperScanner (network port scanning software)
Asset Management: DeepSight (online vulnerability library)

The DTS Database Support Section currently supports industry recognized database packages on the MVS, UNIX and Windows 2000/2003 Operating Systems. The following is a list of those supported packages:
Physically located at Gold Camp Campus

- DataBase Management Systems (DBMS) on UNIX (Solaris):
  - Oracle

Physically located at Cannery Campus

- DataBase Management Systems (DBMS) on UNIX (AIX):
  - Oracle
  - Informix
  - Cache
  - DB2 (UDB).
- MVS System
  - ADABAS
  - DB2
  - IDMS
  - FOCUS
  - Ramis
- Windows 2000/2003
  - SQL Server
  - Oracle

2.3.3 Cost Estimates

Cost estimates are developed for the Customer as requested.

3 STATE DATA CENTER INTERNET/WEB SERVICE STANDARDS

3.1 Explanation of the Service Standard

In today's business market organizations must provide service and product information to a large customer base. To achieve this goal, businesses have moved to Internet/web technology as a solution to their marketing and automation needs. The State Data Center offers a number of services that can provide solutions to meet the business needs of our customers.

3.1.1 Shared Web Hosting Service

In a shared hosting environment, multiple customers share the same server for their web hosting needs. The server hardware, operating system, web software, and network connectivity are maintained by the State Data Center. Site content and customer application design and support are available at DTS published consulting rates. This service provides an economical solution to customers who have simple web hosting needs and where the customer's business requirements do not demand a dedicated environment. Statistical reports are available upon request for a standard fee.

3.1.2 Shared Web Hosting Highlights

- An economical solution for simple web hosting needs
- Ability to scale a solution to the customer's business needs

- The State Data Center is physically secured from the general public to provide extra security
- Base Storage of 250 MB with 10 GB of data transfer per month
- IP addresses and DNS registration are provided (for ca.gov, state.ca.gov, cahwnet.gov domains only)
- Performance monitoring and alerting functionality
- Backup/Restore offsite storage for data recovery
- Anti-Virus protection.
- Restricted FTP access for content management

3.1.3 Shared SQL Hosting Service

This service allows multiple customers to share a single server with their own instance of an SQL database. This service provides an economical solution to customers who have a need for an SQL database, but do not have business requirements that demand a dedicated database environment. The server hardware, operating system, web software, and SQL software are maintained by the State Data Center, while content, customer applications, and database administration are maintained and supported by the customer.

3.1.4 Shared SQL Hosting Highlights

- Site redundancy for failover
- An economical solution for customers who need access to SQL
- Ability to scale a solution to the customer's business needs
- The State Data Center is physically secured from the general public to provide extra security
- Base Storage of 100MB (Over 100MB storage requires an assigned SQL server)
- Anti-Virus protection

3.1.5 Assigned Internet Web Hosting Services

An Assigned Internet Hosting Service provides a dedicated web environment for a customer on either a Windows/IIS or Unix/Solaris/Sun One Enterprise Server environment for a customer. In a dedicated hosting environment, a customer leases an entire physical server (Windows or Unix) or a virtual instance on a Windows server. The server hardware, operating system, and web software are maintained by the State Data Center, while content and customer applications are maintained and supported by the customer. This service provides various options for customers with business requirements needing a dedicated environment. We can also provide for customized web hosting environments based upon the specific technical requirements provided by our customers. Standard statistical reports are available for a standard fee.

3.1.6 Assigned Internet Web Hosting Highlights

- An economical option for customers who require a dedicated web environment
- Ability to scale the solution to the customer's business need
- The State Data Center is physically secured from the general public to provide extra security

- IP addresses and DNS registration are included (for ca.gov, state.ca.gov, cahwnet.gov domains only)
- Performance monitoring and alerting functionality are included
- Backup/Restore offsite storage for data recovery are included
- Anti-Virus protection
- Restricted FTP access for content management

3.1.7 ListServ / Internet Mail Distribution Service

The ListServ/Internet Mail Distribution Service provides the customer with the capability to send out e-mail notifications to a large number of recipients. This service allows you to provide members of an organization with workgroup collaboration, notification of upcoming events, or important news items. ListServ allows you to modify and customize your distribution lists to fit your particular business needs. The server hardware, operating system, and web software are maintained by the State Data Center.

3.1.8 ListServ/Internet Mail Distribution Highlights

- Solution for customers who need to make e-mail notifications to a large number of recipients
- Ability to manage and personalize your list
- Ability to control distribution and subscriptions to mailing list
- The State Data Center is physically secured from general public to provide extra security

3.1.9 Digital Certificates

The State Data Center provides their customers with the ability to request Secure Server IDs. This service provides a means to establish the identity of the server users are trying to interact with over the Internet. Once the user verifies the identity of the server, communication between the user and the target server is encrypted. As a VeriSign® Corporation Registered Authority (RA) for on site administration of 128-bit domestic server certificates, the DTS Cannery Campus has the ability to administer, install, configure, renew and revoke certificates. The ability to quickly respond to a customer's request to revoke certificates provides extra security, should there be a compromise in the client's secure server ID. DTS Gold Camp is not standardized on a particular vendor for digital certificates. Unless a customer explicitly requests a vendor, Gold Camp Procurement Unit will bid for SSL certs and award it to the lowest bidder. Cold Camp currently has at least three different vendor SSL certs.

3.1.10 Digital Certificate Highlights

- A solution for customers whose business requirements call for secure transmissions
- Ability to scale a solution to the customer's business needs
- The State Data Center is physically secured from the general public to provide extra security

3.1.11 Internet Design and Development

The State Data Center offers a variety of consulting services to provide Internet service support. The State Data Center provides application development support for Microsoft environments,

infrastructure support for variety web software like Microsoft Internet Information Services (IIS) 4.0, 5.0, and Microsoft Front Page 2000 for installation, and web site setup. In addition, State Data Center staff can also provide middleware assistance for installation and configuration of IBM's Web Sphere Application Server software, assistance in establishing web communication transmissions to data sources like SQL, Oracle, Informix, and DB2. Customized statistical reporting is available for customers who require additional information not contained in our standard monthly statistical reports. State Data Center staff is also available to make recommendations for solutions to a customer's particular business needs.

3.1.12 Internet Design and Development Highlights

- Application Development in Microsoft environments
- Ability to scale a solution to business needs
- Infrastructure support for a variety of web software
- Knowledgeable staff to assist with developing solutions to meet specific business needs

3.1.13 Data Backup

The State Data Center provides the necessary backups of the web hosting environments in order to guarantee both the integrity of the Customer's data, as well as State Data Center's ability to recover data as needed.

The State Data Center provides enough disk space to preserve a minimum of 31 days of full system backups. In addition, the State Data Center is responsible for monitoring system backup logs to ensure that all backups are successfully completed. If a system back up fails, the State Data Center identifies and corrects the problem to ensure the system(s) is properly backed up.

The State Data Center is responsible for managing and reporting on the following system backup activities:

- Manage backup and file rotation; tapes are scratched after 31 days
- Backing up servers prior to any system maintenance procedure for which there is a potential for data loss

3.1.14 Restore Request Process

- The requestor must obtain authorization from their department's approving authority (identified at service setup).
- Once authorization is received, the requestor contacts their department's help desk to open a help desk ticket. If no departmental help desk function exists, the requestor contacts the State Data Center Help Desk to open a ticket.
- The customer help desk forwards the ticket to the State Data Center Help Desk (if applicable).
- The ticket is assigned to the State Data Center Internet Services Unit.
- If the requested data is onsite at the State Data Center staff restores the requested data.

- If the requested data is not onsite, the data is requested from off site storage through State Data Center Operations. Once the data is received and restored, the customer receives notification within five days. Once the customer is satisfied with the results of the restore, the ticket will be closed.

3.1.15 Operational Recovery

The State Data Center responds to system failures during prime shift in less than four business hours. If the State Data Center has experienced a catastrophic disaster (i.e. destruction of all or part of the State Data Center) then recovery timeframes are reported to the customer as soon as an estimate is available.

3.1.16 Disaster Recovery

For an additional cost, Disaster Recovery plans will be developed with each customer on a case by case basis.

3.2 Roles and Responsibilities

3.2.1 State Data Center Responsibilities

The State Data Center has extensive experience in hosting web sites and web applications, and can provide customers with detailed project cost estimates and project plans for implementation.

State Data Center technical support staff provides the best possible service to meet customers' needs. Once a service is identified by staff and approved by the customer, the State Data Center sets up and configures web services to standards established by the State Data Center. Support and maintenance includes routine operating system and web server software upgrades and regular patch installation and maintenance.

The State Data Center provides maintenance and support of web services once your site is up and running. Support and maintenance includes IIS patch installation and maintenance of the State Data Center standard web services configuration. Maintenance and support agreements become void if the standard configuration of web software has been modified without prior consent of the State Data Center.

3.2.2 Customer Responsibilities

The customer is responsible for providing a detailed project document that outlines the purpose, objectives, and business requirements of the project. The purpose of the project document is to obtain the type of information necessary to determine an appropriate solution. In addition, depending upon the complexity of the hosting requirements, the customer may be required to provide additional design and architectural documentation. The need for additional design and architectural documentation will be at the discretion of the State Data Center. If the State Data Center determines that there is a need for additional information the State Data Center provides an outline for these requirements.

Once the project document is approved by the State Data Center and the customer, the customer receives a draft service request document that provides language regarding the agreed upon services, scope of work and estimated project costs. After the customer reviews and approves the

draft service request document, the customer submits an official service request to the State Data Center unit to initiate the agreed upon work.

Any Modifications, Additions, or Changes must be initiated and conducted through the agreed upon Change Request process.

The customer is responsible for the support and maintenance of all web applications that are not under the maintenance and support of the State Data Center's Internet Services. Standard supported web software is listed under Internet Design and Development Services.

3.2.3 Joint Responsibilities (State Data Center and Customer)

The State Data Center will work with the customer to provide information that will assist the customer to develop a solution that fits within the standard environment.

The State Data Center currently only provides support and maintenance of Microsoft S-IIS 4.0 and 5.0 software that has been installed and configured by the State Data Center. In addition, any change to the original State Data Center standard web software configuration voids State Data Center's support and maintenance. Additional charges will apply if State Data Center staff is required to reconfigure or reinstall web software to standard configurations.

3.3 Pricing

Rates are available in the DTS Rates Schedule

(Note: The total setup charge is based upon the time required to complete the initial configuration, setup, and any necessary design and development activities. The State Data Center can provide a quote for the setup charge after analysis of your proposed web hosting project.)

3.3.1 Shared Web Hosting Service

A one time charge is incurred for initial configuration, setup and any additional Design and Development activities. Additional storage and data transfer charges are incurred at incremental levels.

3.3.2 Shared SQL Hosting Service

The standard unit of measurement is one instance of an SQL database. One time charges are incurred for initial configuration, setup and any additional Design and Development activities.

3.3.3 Assigned Internet Web Hosting Service

The standard unit of measurement is one web server or one virtual instance on a Windows server. A one time charge is incurred for initial configuration, setup and any additional Design and Development activities.

3.3.4 ListServ Internet Mail Distribution Service

The standard unit of measurement is one list. Each list owner has the ability to control when a distribution occurs and has the ability to control subscriptions to the mailing list.

3.3.5 Digital Certificates

The unit of cost is one digital certificate. Installation and configuration charges are charged at State Data Center's standard Internet Design and Development fee.

3.3.6 Internet Design and Development

Internet design and development charges are marked at an hourly rate.

4 STATE DATA CENTER MAINFRAME APPLICATION HOSTING

4.1 Explanation of the Service Offering

4.1.1 Statement of Service

Broadly available software applications are a vital component of many businesses. Ensuring that these applications are hosted in a reliable, secure, and technologically up-to-date environment is, for many organizations, difficult, expensive, and a drain on technical support staff. The State Data Center offers extensive, secure processing, monitors computing availability and performance, and provides backup and recovery capabilities.

The State Data Center provides software application hosting on mainframe computers running the OS/390 (soon to be z/OS) operating system (OS). Our mainframe computers are located in our secure, environmentally controlled raised floor computer room. The State Data Center provides full power system redundancy and a fire suppression system.

4.1.2 Service Offering Highlights

The State Data Center Mainframe Application Hosting includes the following:

- Hardware procurement, installation, and maintenance for mainframes
- Software procurement, installation, and maintenance for mainframes (operating system, system utilities, database, and web software)
- Performance monitoring
- Network connectivity
- Environmentally controlled secure facility
- Reliable power with full uninterruptible power supply (UPS) and generator backup
- Halon fire suppression system
- System backup and recovery
- Security systems including virus protection, data encryption, and intrusion detection

4.1.3 System Response Time

Both the Customer and the State Data Center monitor the health of the system. Various factors determine the user's wait-time when executing a command from their keyboard/mouse. These factors include the configuration of individual customer networks, the speed of the desktop processor, the amount of available RAM on a desktop, and the type of software package executed. These factors can vary from one desktop to the next so system response times will also

vary. Additional functionality and configuration of customer LANs can also impact system response time.

The State Data Center maintains service level objectives for system response time. In addition, the State Data Center works with the customer to resolve response time issues as appropriate.

4.1.4 System Monitoring

Operational considerations to be included in the State Data Center system monitoring are: a daily check of the backup logs to insure system backups have executed properly, and ongoing monitoring of system availability and system performance. If any problems or issues are discovered, the State Data Center contacts the customer to coordinate the implementation of a problem solution.

4.1.5 Operations Support and Command Center

The State Data Center is staffed 24 hours per day, seven days a week and provides system monitoring and availability support for the mainframe environment, manages tape handling, and manages customer backups. The State Data Center provides customer feedback according to the Severity Code Definitions outlined in Appendix B.

4.1.6 Data Backup

The State Data Center performs the necessary system backups for the mainframe environment in order to guarantee both the integrity of the customer's data, as well as the State Data Center's ability to recover that data as needed. The State Data Center retains 31 days of full system backups.

Mainframe backups prior to any system or application maintenance procedure may be requested.

4.1.7 Restore Request Process

File and disk restoration from tape backup is reserved for disk failure, disaster recovery, and loss of data integrity where the customer and State Data Center determine a restore is the most efficient method of restoring data integrity. The requestor must obtain authorization from their department's approving authority. Once authorization is received, the requestor contacts their department's help desk to open a help desk ticket. If no departmental help desk function exists, the requestor contacts the State Data Center Help Desk to open a ticket. The customer help desk forwards the ticket to the State Data Center Help Desk (if applicable).

4.1.8 Operational Recovery

The State Data Center responds to system failures immediately. The State Data Center maintains a 24 hour 1st level help desk that alerts key system support staff of any unplanned outage to ensure timely resolution.

4.1.9 Disaster Recovery

For an additional cost, Disaster Recovery plans will be developed with each customer on a case by case basis.

4.1.10 Security

The State Data Center takes all necessary precautions to protect mainframe computers from unauthorized access including modification, deletion, or disclosure of the databases and operating systems.

The State Data Center and the customer are responsible for ensuring the protection of confidential data stored and transmitted. Additionally, the State Data Center performs logging and tracking of security events should they occur.

The customer agrees to exercise reasonable efforts to safeguard the following information:

- Specific version information of the systems' firmware, operating system, and applications in order to minimize the potential exploitation of vulnerabilities prior to release and application of service packs/fixes
- Account names/passwords
- IP addresses/system names

The State Data Center and the customer are responsible for notifying the appropriate security representative (usually the Information security Officer) of any suspected unauthorized access.

The State Data Center and the customer are responsible for maintaining hardware and software at vendor supported levels. Customers are responsible for maintaining application software at the supported levels of the system software. If customers delay in updating application software, additional support costs will be incurred.

The State of California and the State Data Center's customers require that the State Data Center maintain IT security that protects the entire data center and all of its customers from unauthorized intrusions. Mainframe Application Hosting customers are expected to observe the various IT security-related best practices, standards, and policies in force within the State Data Center including the security guidelines outlined by the International Standards Organization section ISO-17999.

Customers not in compliance with the State Data Center's security guidelines subject the State Data Center and its other customers to unnecessary security risks and consequences. The State Data Center may take remedial action or discontinue services to Application Hosting customers that disregard the security guidelines. Specific IT security-related guidelines for Application Hosting customers are contained within the Paragraph 4.1.10.1, Operations and Systems Security below.

All Application Hosting customer service requests and project changes must include a review and approval by the customer's Information Security Officer (ISO) and the State Data Center's ISO.

4.1.10.1 Operations and Systems Security

Mainframe Application Hosting customers are responsible for the following IT security areas:

- Maintain up-to-date application and patch upgrades. All application and patch upgrades are tested on a comparable test environment.

- Work in conjunction with State Data Center Security Staff using an intrusion detection system (IDS) and perform testing as deemed necessary (host IDS or file integrity checking)
- Work in conjunction with State Data Center Security Staff providing pre-production and subsequent security vulnerability scanning and analysis of hosted applications
- Adhere to current DTS security guidelines regarding foreign connections into the DTS trusted network. (These practices include, but are not limited to, remote administration, Telnet, and FTP.)

4.2 Roles and Responsibilities

Setting up and supporting a reliable and secure software application-hosting environment can be a daunting task. The State Data Center's experience with other mainframe customers affords us with the expertise to help customers deploy their application solutions.

The State Data Center's technical support staff sets up and configures the mainframe to integrate efficiently with each customer's network configuration and user population size. The State Data Center continually analyzes the hosting infrastructure to ensure operational integrity and the ability to grow as needed.

4.2.1 State Data Center Responsibilities

4.2.1.1 Provide Performance Analysis

- Track resource utilization
- Provide maintenance of monitoring and data gathering tools
- Notify the customer of storage capacity and/or performance issues the State Data Center discovers

4.2.1.2 Provide Server OS Support

- Perform installation and maintenance of Operating System (OS) and related utilities
- Troubleshoot mainframe hardware and OS
- Backup and restore the OS

4.2.1.3 Provide System Database Support

- Perform installation and maintenance of database software
- Develop and maintain database to all OS interfaces
- Provide general system troubleshooting
- Provide application data restoration and recovery

4.2.1.4 Provide Enterprise Storage Support

- Provide installation and maintenance of storage subsystem
- Provide installation and maintenance of enterprise storage backup solutions
- Provide storage system troubleshooting

4.2.1.5 Provide Network Connectivity

- Establish connectivity from the mainframe to an existing DTS/customer network
- Establish isolated connectivity and firewall protection (purchased separately as part of DTS's network access service offering).

4.2.2 Customer Responsibilities

4.2.2.1 Provide Customer System Administration

- Act as the primary contact for the customer when contact by State Data Center support staff is needed
- Participate in development/maintenance of OS to OS interfaces
- Provide user administration

4.2.2.2 Provide Application Database Support

- Act as the primary contact for the customer when contacted by State Data Center support staff is needed
- Provide database development and support

4.2.2.3 Provide Application Support

- Provide development and maintenance of the application
- Provide development and maintenance of the application to all OS interfaces

4.2.3 Joint Responsibilities (State Data Center and Customer)

- Provide monitoring and notification on system availability, performance, storage limitations when the mainframe is nearing capacity, and other technical issues
- Provide application data restoration/recovery

4.3 Pricing

4.3.1 Basic Service Offering Pricing

Rates are available in the DTS Rates Schedule
http://www.dts.ca.gov/customers/rates

4.3.2 Options

The list below displays the software, languages, packages, etc. that are provided:

Network Software:

ACF/NCP
SSP
Network Performance Monitor - full product
Network Terminal Option
NCCF, NPDA and NLDM, modules within Tivoli Netview for mainframe
ACF/VTAM

IND$FILE

Programming Languages:

- High Level Assembler
- IBM SDK For z/OS Java 2 Technology Edition
- COBOL for OS/390 and VM
- VS COBOL II Compiler
- VS COBOL II Subroutines
- C/C++
- XPEDITER/TSO COBOL debugging tool
- VS FORTRAN Compiler
  - and Libraries
  - and Interactive Debug
- PL1 OPTIMIZING COMP.,LIB. AND INTERACTIVE TEST
- LE for OS/390 and VM
- NATURAL
  - Super NATURAL
- ADS/
- RAMIS
  - MARVEL
  - RPI
  - ADABAS Interface

TSO Support Packages:

- BookManager/Read
- FileAid/XE
- Graphical Data Display Manager (GDDM)
- Interactive System Productivity Facility
  - ISPF Dialog Manager
- IOF
- PAN TSO
- Panvalet/SPF Option
- PDSMAN
- PLI CHECKOUT COMPILER
- PL/I LANG. CONSTRUCTION PREPROCESSOR
- PMF (Print Manag. Facility)
- PSAF (Print Serv. Acc. Fac.)
- Screen Definition Facility II
- TSO DATA UTILITIES
- VS APL
- VS COBOL II COBTEST
- VS FORTRAN INTERACTIVE DEBUG
- VTAM Printer Support system (VPS)
- XPEDITER/TSO (COBOL debugging tool)

CICS Support Packages:

- CICS/TS

ABEND AID
INTERTEST
XPEDITER
ASSIST/GT
IPCP
OMEGAMON II CICS
OMEGAVIEW
SUPEROPTIMIZER
VPS
VMCF
VPSPRINT
RPT/BROWSE
DRS
TPX
CONNECT:DIRECT
DYNAPRINT
HIPERSTATION
SPY
ROPE

Business Intelligence Software:

IMSL
SAS (Integration Technologies, CONNECT, IntrNet, Metadata Server, Base, Access/ADABAS & DB2, AF, ASSIST, ETS, FSP, GRAPH, IML, QC, SHARE, STAT, Stored Process Server, Workspace Server)

Data Base/Data Management Support:

EDA
DB2 for OS/390
CA-PAN/SQL
!DB/Explain(!Candle)
DpropR Capture and Apply for MVS
File-AID For DB2 (w/xpediter ext.)
File-AID/RDX For DB2
Insight/DB2
KBMS/DB2
NATURAL DB2
Omegamon II for DB2
PLATINUM Product Suite
PLATINUM Compile/PRF
PLATINUM Database Analyzer
PLATINUM Fast Unload
PLATINUM Execution Facility
PLATINUM Governor Facility
PLATINUM Plan Analyzer

- PLATINUM RC/Compare
- PLATINUM RC/Migrator
- PLATINUM RC/Query
- PLATINUM RC/Secure
- PLATINUM RC/Update
- PLATINUM Recovery Analyzer
- PLATINUM Report Facility
- PLATINUM SQL-Ease

- QMF/MVS
- Knowledge Xpert for DB2(RevealNet)
- RLX/SQL
- RLX/CLIST
- RLX/ISPF
- RLX/NET
- RLX/TSO
- Smart/RESTART
- Smart/RRS
- STROBE For DB2
- Thread/SENTRY
- Thread/STOPPER
- VisualAge Host Services

ADABAS

- AOS
- APAS/INSIGHT
- NATIVE SQL
- ENTIRE
  - ENTIREX BROKER
  - ENTIREX Security
  - NETWORK MAINFRAME
- NATURAL Product Line
  - CON-NECT
  - CON-NECT SNADS LINK
  - CON-FORM
  - CONSTRUCT
- NATURAL
- NATURAL Advanced Facilities
- NATURAL Connection
- NATURAL DB2
- NATURAL Security
- NATURAL VSAM
- PREDICT (Data Dictionary)
- PREDICT Application Control
- STROBE For Adabas/Natural
- Super NATURAL
- Simply Natural

Chart

IDMS
ADS/O (see Programming Languages)
IDMS Tools
DBSTATS
FAST/ACCESS

Misc:
FOCUS
RAMIS (see Programming Languages)

Report Preparation Packages:
EASYTRIEVE PLUS
EASYTRIEVE UTILITIES
NATURAL (see languages)
PANAUDIT PLUS
PANAUDIT
RAMIS (see languages)
RESULTS (DYL280 II)
TPL/PCL

Other Support Packages:
ABENDAID
ADRS II
Comparex
Compuware ECC (Shared Services)
DCD III
Deliver (formerly Express Delivery)
DMS/OS see Sams:DISK
Document Composition Facility (SCRIPT)
Execution Scheduling Processor (ESP)
Encore (restart/rerun)
FATS/FATR
FDR/DSF
FileAid/XE
HFDL (Xerox Host Forms Defn Lang)
HourGlass 2000
IAM
Interactive Instructional Presentation System
IrmaLink
JCLFLOW
JobScan
KOMPACTOR
LSTCAT (listcat plus)
MICS

MIM (Multi-Image Manager)
OGL/370 (IBM Overlay Gen Lang)
OMEGAMON/MVS
PANVALET
PDSMAN
PKZIP (compression package)
PPFA/370 (Page Prt Format Aid)
PSF (Advanced Function Printing)
Quickref
OS/390 Security Server (RACF)
RESOLVE
RMF
RPLUS (UCCR+)
Sams:DISK (formerly DMS/OS)
BrightStor CA-Compress Data Compression.
SMP/E
SSANAME3
STROBE
SYNCSORT
TMS (CA-1) Tape Management System
TSA
TSO-MON
View (formerly SAR)
- Extended Retention Option
- CICS interface
- SAR/PC for DOS
- View Workstation

Vanguard RACF Administrator (VRA)
Vanguard RACF Security Reporter VSR)

4.3.3 Cost Estimates

Cost estimates are developed for the Customer as requested.

5 BEST PRACTICES, LEGAL REQUIREMENTS AND OTHER STANDARDS

5.1 General

The State Data Center requires that all projects comply with the following IT Security Standards as applicable. All projects must comply with the ISO 17799 Standard. The State Data Center supports the IT security principles of Confidentiality, Integrity, and Availability. To that end, the State Data Center requires that all projects operating in, maintained by, or hosted by State Data Center follow the standards set forth in this document.

5.2 Legal

Projects must comply with existing and future local, State, and Federal laws as applicable. Projects must conform to all applicable California State Administrative Manual (SAM) regulations. Laws include but are not limited to:

- U.S. Privacy Act of 1974
- U.S. Copyright Act of 1980 Title 17
- Health Insurance Portability and Accountability Act (HIPAA)
- Digital Millennium Copyright Act (DMCA)
- Uniform Trade Secrets Act
- Electronic Communications Protection Act
- California Civil Code 1798

5.3 Systems

Projects must meet current and future State Data Center requirements for systems. All systems must comply with State Data Center IT security policies.

5.3.1 Supported Environments

State Data Center requires that all projects conform to current State Data Center hardware and software standard supported environments. State Data Center recommends deploying on standard, supported infrastructure. Hardware includes client, server, mid-range, mainframe, network, telephony, and associated equipment. Software includes applications, utilities, operating systems, databases, macros, and scripts. State Data Center may, at its discretion, agree to install, configure, support, and/or maintain hardware and/or software that falls outside the scope of its expertise and/or standards.

5.3.2 Software Patches

All commercial off-the-shelf (COTS) and proprietary software must be maintained at current patch levels. Our Triage and System Maintenance Processes allow for this type of stabilization. Software includes applications, utilities, operating systems, databases, macros, and scripts. Patches must be fully tested in a similar environment before implementation on production systems.

5.3.3 Availability

Systems maintained by State Data Center are required to follow current and future Preventative Maintenance (PM) windows. Systems must be configured to allow for PM activities. Systems must be designed to provide the level of availability required by the customer.

5.3.4 Host/System Hardening

All systems must comply with the latest applicable host hardening best practices as well as any specific requirements for functioning within the DTS network. Unnecessary services must be turned off. Unnecessary software and/or services must be completely removed from the systems

if possible. Hardening practices include but are not limited to the following and may come from other "best practices" sources than the ones listed:

- Unix

  http://www.cert.org/tech_tips/usc20_full.html
- Microsoft

  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/hardsys/default.asp
- Cisco

  http://www.cisecurity.org/bench_cisco.html
- Others

  http://www.sans.org/score/firewallchecklist.php

5.3.5 Vulnerability Assessments

Vulnerability Assessments are performed on a daily and weekly basis. All systems must undergo a security vulnerability assessment prior to going into production. After the initial vulnerability assessment is completed, State Data Center requires that all high and medium vulnerabilities be rectified or mitigated. A follow-up vulnerability assessment must occur prior to the system going into production to ensure that all identified high and medium vulnerabilities have been resolved and that no additional high or medium vulnerabilities are present.

All low vulnerabilities must be rectified or mitigated within one (1) month of the initial vulnerability scan. The State Data Center performs periodic vulnerability scans of all systems.

5.3.6 Baseline

All systems must meet current State Data Center baseline configurations as described in existing State Data Center documentation.

5.4 Data

Projects must meet current and future State Data Center requirements for data. All projects must comply with State Data Center IT security policies.

5.4.1 Data Classification

State Data Center classifies data according to its data classification standards. At the minimum, the data classification must comply with SAM and any applicable laws.

http://csrc.nist.gov/cc/Documents/CC%20v2.1/p2-v21.pdf

5.4.2 Encryption

State Data Center requires encryption to ensure data security based on the data classification level as well as mandated by law (i.e., HIPAA, SB1386, SB1, AB700 and any other law/legislation that involves data security in transit and in storage). State Data Center advocates the use of the Advanced Encryption Standard (AES) and Secure Socket Layer (SSL) technologies per recommendations from the Internet Engineering Task Force (IETF) and the

Nation Institute of Standards and Technology (NIST). The data classification and/or legal requirements determine if data must be encrypted or not.

http://csrc.nist.gov/CryptoToolkit/aes/index.html

5.5 Applications

Projects must meet current and future State Data Center requirements for applications. All projects must comply with State Data Center IT security policies.

5.5.1 Patching

State Data Center requires timely patching to maintain the operational availability, confidentiality, and integrity of information technology systems. In order to manage the growing number of patches and the complexity inherent in the network, the State Data Center instituted the Security Patch Management Process. General patching information can be found at:

http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf

5.5.2 Availability

Applications running on systems maintained by State Data Center are required to follow current and future Preventative Maintenance (PM) windows. Applications must be designed to allow for PM activities. Applications must be designed to provide the level of availability required by the customer.

5.5.3 Code and Code Review

Proprietary source code (written computer instructions) must follow current security design standards, including ISO 17799. Based on data classification levels, proprietary source code must also comply with applicable laws. Additionally, it must be examined for deficiencies in security, reliability, and operations during the development process.

http://www.itl.nist.gov/div897/sqg/pubs/publications.htm

5.5.4 Application Security

State Data Center requires measures be implemented to ensure the confidentiality, integrity, and availability of data and processes within an application. State Data Center requires projects comply with existing access control mechanisms.

http://www.cio.gov.bc.ca/itsp/sec66.htm

5.6 Authentication

Projects must meet current and future State Data Center requirements regarding authentication. All projects must comply with State Data Center IT security policies.

5.6.1 SSL/IPSec

State Data Center requires Secure Sockets Layer for distributed and n-tier applications, for providing authorization in heterogeneous environments, and in securing data transactions and remote operation control. SSL provides confidentiality, integrity, authentication and non-

repudiation. Some instances of SSL may be required by law. IPSec may be substituted where applicable.

5.6.2 Certificates

State Data Center requires the use of digital certificates as needed. Certificates must be issued by a credible certification authority (CA).

5.6.3 File Transfers

All file transfers must occur via a Secure FTP, Secure Shell Copy facility, or other secure method. User names and passwords must not be transferred via plain text. Some file transfers may be governed by additional laws and must comply with these laws. Encryption must comply with current and future State Data Center policy and/or applicable laws.

5.6.4 Access Controls

State Data Center requires access controls in compliance with ISO 17799. Projects must define access control policy and rules, user password use and management, node authentication, and system access monitoring. State Data Center strictly limits and controls remote and mobile computing. Projects must specify the business need to include wireless computing. Wireless justifications must include detailed security measures to ensure the confidentiality, integrity, and availability of the project systems, network, and data as well as the entire State Data Center and its customers.

http://www.iso17799software.com/7799part1.htm

5.6.5 Encryption

If data has been classified as “sensitive” State Data Center recommends encryption as the way to protect the data. State Data Center advocates the use of the Advanced Encryption Standard (AES) and Secure Socket Layer (SSL) technologies per recommendations from the Internet Engineering Task Force (IETF) and the Nation Institute of Standards and Technology (NIST). Legal requirements and other policies may dictate the use of encryption. Access to systems via remote technologies must occur through SSH or other secure method.

http://csrc.nist.gov/CryptoToolkit/aes/index.html

5.7 Operations/Production Control

Projects must meet current and future State Data Center requirements for operations and production control. All projects must comply with State Data Center IT security policies.

5.7.1 Availability

Projects running on the State Data Center maintained network infrastructure are required to follow current and future Preventative Maintenance (PM) windows. Network design must allow for PM activities. Applications must be designed to provide the level of availability required by the customer.

5.7.2 Change Management

State Data Center requires compliance with its Change Management process. All system changes must be researched, tested, validated, and documented prior to execution. Due to its potential disruption to the system, the State Data Center enforces strict logical and physical access controls to this process.

5.7.3 Staffing

State Data Center uses separation of duties which divides roles and responsibilities so that a single individual cannot subvert a critical process. State Data Center requires projects to comply with this model. Furthermore, State Data Center grants users only that access they need to perform their official duties. Finally, employees are trained in the computer security responsibilities and duties associated with their jobs.

5.7.4 Maintenance Plan

All projects must include a maintenance plan. This plan must comply with existing and future State Data Center policy, guidelines, and practices including but not limited to: Change Management, Backup Processes, and Patch Management. Applications and/or systems not supported by State Data Center must include user administration and access privileges processes. State Data Center requires periodic security audits for systems and applications regardless of whether State Data Center maintains them or not.

5.7.5 Service Level Agreement

State Data Center requires a service level agreement between itself and any vendor providing services through the DTS network. Defined service levels provide a basis for measuring the delivered services and are useful in anticipating, identifying, and correcting problems. An SLA should contain a definition of service expectations which is of an acceptable high standard and achievable within the budget allocated.

5.7.6 Patching

State Data Center requires timely patching to maintain the operational availability, confidentiality, and integrity of information technology systems. In order to manage the growing number of patches and the complexity inherent in the network, the State Data Center instituted the Security Patch Management Process. General patching information can be found at:

http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf

5.7.7 Multi-Environment Support (Test, Development, and Staging Systems)

State Data Center requires separate test, development, and staging systems for all projects. This helps ensure that modifications do not affect production systems until those modifications have been tested.

5.7.8 Disaster Recovery

State Data Center requires projects comply with existing and future disaster recovery plans, business continuity plans and other processes as required by law. Project solutions must include

a complete business continuity plan and solution specific to the project itself including but not limited to:

- A listing and classification of threats to the solution.
- Plans for disaster recovery, tailored to each listed threat.
- Systems and resources, as appropriate, necessary to implement and execute each disaster recovery plan.
- Plans and scheduling for plan testing and maintenance.

5.7.9 Account Management

State Data Center requires a means to manage the creation, deletion, and modification of user accounts. This includes both operating system and application-level accounts. Accounts must be classified according to the resources required by each different kind of user. Use of accounts must be enforced with appropriate access control techniques. Projects must include an explanation of the different kinds of user accounts and directions on how to manage them.

5.7.10 Availability

Systems maintained by State Data Center are required to follow current and future Preventative Maintenance (PM) windows. Systems must be configured to allow for PM activities. Systems must be designed to provide the level of availability required by the customer.

5.7.11 Independent Verification and Validation

State Data Center periodically conducts independent third party audits of our IT Security Program – previous audits have been conducted by State Departments as well as private businesses) . State Data Center requires independent verification and validation (IV&V) of a project's IT security components. The IV&V results assure that the security features of the delivered solution meet the specified requirements and applicable laws. The level and scope of the IV&V will be specified by State Data Center on a per-proposal basis.

5.8 Architecture

Projects must meet current and future State Data Center requirements for system architecture. All projects must comply with State Data Center IT security policies.

5.8.1 Physical Security

State Data Center requires that secure areas be protected by appropriate entry controls. Account shall be taken of relevant health and safety regulations and standards.

Equipment shall be physically protected from security threats and environmental hazards. Equipment shall be protected from power failures and other electrical anomalies. A suitable electrical supply shall be provided that conforms to the equipment manufacturer's specifications. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. Equipment shall be correctly maintained to ensure its continued availability and integrity. The use of equipment outside of State Data Center premises for information processing shall be approved by the appropriate management. The security provided shall be equivalent to that for on-site equipment used for the same purpose, taking into

account the risks of working outside State Data Center's premises. Storage devices containing sensitive or confidential information shall be physically destroyed or securely overwritten. All items of equipment containing storage media, for example, fixed hard disks, shall be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal.

Information and information processing facilities shall be protected from disclosure to, modification of or theft by unauthorized person, and controls should be in place to minimize loss or damage.

See ISO 17799

5.8.2 Application Security

State Data Center requires that application security, regardless of the application or the platform on which it runs, must be implemented at the design stage. State Data Center requires compliance with ISO 17799 and other industry best practices. Applications must protect the information relevant to the system and protect other information that is stored on the same platform that could be compromised by manipulation of the same system. State Data Center requires that application security relate closely with data classification. Some laws may apply.

APPENDIX A - DEFINITION STATEMENTS

Assigned Hosting
Assigned hosting is the business of hosting web sites and applications on a dedicated server for customers. The customer has the option of leasing a web server from the State Data Center for their specific web hosting business needs.

Assigned SQL Hosting
Assigned SQL hosting is the business of hosting an SQL database on a dedicated server for customers.

Asynchronous Transfer Mode
ATM – a dedicated connection switching technology that organizes digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology.

Base Storage
Base storage is the amount of hard disk storage included in the web hosting base price.

Channel Service Unit/Digital Service Unit
CSU/DSU - a hardware device that converts digital data frame from the communications technology used on a LAN into a frame-appropriate to a WAN and vice versa.

DASD
DASD is an acronym which stands for Direct Access Storage Device. A type of storage device, such as a magnetic disk, in which bits of data are stored at precise locations, enabling a computer to retrieve information directly without having to scan a series of records.

Data transfer
Data transfer is the amount of data transferred to and from a web site.

Demilitarized Zone
DMZ - a small network inserted as a "neutral zone" between DTS's Intranet and the outside public network.

Digital Subscriber Line
DSL – a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines.

DNS registration
DNS stands for Domain Name Services. The DNS registration of a web site name puts the web site's address in a directory that allows users to find the web site on the Internet based upon its web site address.

Domain
The domain is the text name used to locate a web site on the Internet.

Enterprise Storage
Enterprise storage is a centralized repository for business information that provides common data management and protection, as well as data sharing functions, through connections to numerous (and possibly dissimilar) computer systems.

First Level Help
First Level Help is the initial contact point that computer system end users call when they need assistance with a software application, computer hardware, or other problem. In relation to DTS service standards, the First Level Help is usually the DTS customer's own help desk. If the customer does not have a help desk, the First Level Help is the State Data Center Help Desk.

Frame Relay
A shared, packet oriented network provided by telephone carriers.

GB
GB stands for gigabyte. A gigabyte is a unit of measurement for computer storage capacity equaling approximately one billion bytes.

Halon
Any of several halocarbons used as fire-extinguishing agents. Halon is used in computing environments because it causes less damage to electronic equipment than other fire-extinguishing agents.

Intrusion Detection System
IDS - used to detect unauthorized activities on the DTS network.

IIS
IIS stands for Internet Information Server. IIS is the Microsoft software for Internet web servers that allow web sites to be presented to users that request them.

Internet Protocol
IP - a protocol by which data is sent from one computer to another on the Internet.

IP address
IP stands for Internet Protocol. An IP address is a numeric identifier for a computer on a Transmission Control Protocol/Internet Protocol (TCP/IP) network.

LAN
A local area network (LAN) is a group of computers and associated devices that share common communications line(s) and typically share the resources of one or more servers within a small geographic area (for example, within an office building). Usually, the server(s) contains applications and data storage that are shared in common by multiple computer users.

ListServ
ListServ is the Lsoft International software application for e-mail distribution services.

Mainframe Systems
In the beginning, all computers were mainframes since mainframe was just another term for the cabinet that held the CPU (Central Processing Unit). Mainframe means large scale computer, and it also implies the technical expertise necessary to run it.

Mainframe operating systems can extend the highest quality security, scalability and performance for enterprise transactions and data to new applications, including Internet and Java-enabled applications.

Metropolitan Area Network
MAN – a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large LAN, but smaller than the area covered by a WAN.

MB
MB stands for megabyte. A megabyte is a unit of measurement of computer storage equaling approximately a million bytes.

Midrange Systems
Midrange systems are medium-sized computer systems that provide the functions of a mainframe but on smaller, more cost effective units.

Network Address Translation
NAT – a service that translates an internal private address to a public address to enable connectivity outside of the DTS network.

Operating System
An operating system (often abbreviated as "OS") is the program that, after being initially loaded into a computer by a startup program, manages all the other programs in a computer.

POP
Point of Presence (POP) – an access point to the Internet.

Router
A router is a network device that is used in DTS's network to interconnect remote and central network components.

Second Level Help
Second Level Help is the contact point that a State Data Center customer's Help Desk (First Level Help) calls when they need assistance with a problem that they have determined is the responsibility of the State Data Center

Shared SQL Hosting
Shared SQL hosting is when multiple customers share the same server resource with their own instance of an SQL database.

Shared Web Hosting
Shared web hosting is when multiple customers share the same web hosting environment for their web hosting business needs.

SQL Database
A Microsoft database that supports Structured Query Language (SQL).

Secure Socket Layer
SSL – a commonly used protocol for managing the security of a message transmission on the Internet.

T1
A data service line that provides speeds of 1.544 MBPS and is often partitioned into 24 DS-0 channels.

T3
A data service line that provides speeds of 45 MBPS.

Transmission Control Protocol/Internet Protocol
TCP/IP – a network protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems.

Third Level Help
Third Level Help is the contact point that the State Data Center Help Desk calls when they need assistance resolving a problem that they have determined is the responsibility of a particular State Data Center service area.

Uninterruptible Power Supply
An uninterruptible power supply (UPS) is a device that allows a computer or computers to keep running for at least a short time when the primary power source is lost. It also provides protection from power surges.

V.90
A standard for transmitting data downstream to modems at 56 kbps.

Virtual Private Network
VPN – a way to use public telecommunications infrastructure, such as the Internet, to provide remote offices or individual users with secure access to DTS's network.

Voice over Internet Protocol
VoIP – a term used in IP telephony for a set of facilities for managing the delivery of voice information using the Internet Protocol.

Wide Area Network
WAN – a network service that provides statewide transport solutions.

Web Hosting
Web hosting is the business of housing, serving and maintaining information for one or more web sites.

APPENDIX B - STATE DATA CENTER HELP DESK

State Data Center Help Desk Process

The State Data Center Help Desk is staffed Monday-Friday, 5:00 a.m. – 10:00 p.m., and Saturday, 7:00 a.m. – 12:00 p.m., and available for support and troubleshooting 7 days a week, 24 hours a day.

State Data Center Issue Reporting Process

- The customer contacts the State Data Center Help Desk
- A trouble ticket is opened and routed to the appropriate business area if the issue is not immediately resolved
- The State Data Center staff works to resolve the issue and updates the trouble ticket
- The Help Desk keeps the customer updated with the issue status
- When issue is resolved, staff from the business unit working the issue notifies the Help Desk
- The customer is notified about ticket resolution, and the ticket is closed if the customers has no additional concerns

The Help Desk levels are defined as follows:

First Level: Customer end user or Customer Help Desk
Second Level: The State Data Center Help Desk
Third Level: State Data Center technical support

Help Desk Severity Code Definitions

The matrix shown below contains the definitions of trouble ticket severity codes and the required response times for accepting trouble tickets and providing customer feedback on the problem resolution. Severity levels are assigned by State Data Center Help Desk at the time a trouble ticket is reported.

SEVERITY LEVEL	IMPACT/DESCRIPTION	RESOLUTION
Severity One	Severe impact to Customer site. For example: - Server outage - Database unavailable	The Help Desk opens or accepts ticket within 15 minutes A Technician responds to dispatch within 15 minutes and gives an estimated time of arrival (ETA) and problem description to the Help Desk within one hour. The Help Desk updates the ticket. Technicians continue to provide verbal updates to the Help Desk every 60 minutes. The Help Desk notifies the customer of ticket status every hour via phone or other negotiated means. Technicians update the ticket within one business day of problem resolution.
Severity Two	Operations continuing but greatly degraded; multiple users affected. For example: - Degradation of mission critical application	The Help Desk opens the ticket within 30 minutes. A technician responds to dispatch within one hour and gives an ETA and problem

	- Intermittent file server problem	description to the Help Desk within one hour. Technicians continue to provide verbal updates to the Help Desk daily. The Help Desk notifies the customer of ticket status daily. Technicians update the ticket within one business day of problem resolution.
Severity Three	Operations affected less than once a week; single user affected. For example: - Problems that degrade but do not prevent accessibility/usability - Workstation outage with other workstations available - Degradation of non-critical application	The Help Desk opens a ticket within one hour. A technician responds to dispatch within two hours and gives ETA and problem description to the Help Desk within one day. The Technician continues to provide verbal updates to the Help Desk daily. The Technician updates the ticket within one business day of problem resolution.
Severity Four	Minimal impact to operations. For example: - Problem with low impact to user - Scheduled outage	The Help Desk opens a ticket within two hours. A technician responds to dispatch within four hours and gives an ETA and problem description to the Help Desk within one day. The technician continues to provide verbal updates to the Help Desk every other day The Help Desk notifies the customer of ticket status weekly. The technician updates the ticket within one business day of problem resolution.

APPENDIX C - AVAILABILITY AND SUPPORT

System Availability

System availability refers to the scheduled daily hours of operation for this service. System availability is divided into three categories: (1) Normal Hours of Operation; (2) Off-Hours of Operation; and (3) Planned System Outages.

Normal Hours of Operation

Normal hours of operation are Monday through Friday, 7:00 AM to 5:00 PM excluding holidays.

Off-Hours of Operation

Off-Hours of Operation are Monday through Friday, 5:01 PM to 6:59 AM and Saturday, Sunday, and holidays, 7:00 AM to 6:59 AM.

Planned System Outage

The following are planned system outages:

- System conversions and hardware and software upgrades or replacements;
  - o System service is preceded by at least two weeks advance written notice to the customer;
  - o System changes are tested in a test environment for a minimum of 30 days; and
  - o System service is scheduled using the State Data Center change management process.
- Preventive Maintenance (PM) is performed every Sunday evening and Monday morning of each month, between 11:30 p.m. and 4 a.m. However, if a regularly scheduled PM falls on a Monday State Holiday, it is postponed until the following Tuesday during the same timeframe. The State Data Center publishes a Preventive Maintenance (PM) Schedule via the change management process. PM is designed to provide regular system service with minimal system outage.
- Quarterly Extended Preventative Maintenance is performed every third (3rd) Monday in January, April, July and October between 12 midnight and 4 a.m. However, if the proposed day falls on a Monday State Holiday, it is postponed until the following Tuesday during the same timeframe. During this period, maintenance occurs when maintenance activities cannot be accommodated within the normal scheduled timeframes. Customers are notified when extended maintenance will occur through the State Data Center Change Management Request (CMR) process.
- System backups are usually run nightly between 6:00 PM and 6:00 AM;
- Critical Security Patches requiring short notice.

Miscellaneous System Maintenance

- **Emergency maintenance** occurs when critical system maintenance must be implemented. Customers are notified when an emergency maintenance situation must be implemented.
- Other maintenance, such as malfunctioning equipment (router) outside of the normal maintenance schedule, is performed at mutually agreed-upon times with the customer.

Specific objectives are listed in this section regarding the total amount of time the State Data Center guarantees the system to be available within those hours. This guarantee pertains to those system components covered under this service offering only. The "down time" of any components covered under this service offering that become inoperable during guaranteed hours counts against the State Data Center system availability guarantee. If any other components necessary for delivery of this service that are not included in this service offering become inoperable during guaranteed hours and the State Data Center covered components remain operable, that "down-time" does not count against the State Data Center system availability guarantee. For example:

- Should a county site printer breakdown during the printing of reports or warrants, State Data Center is not responsible for the inability to deliver said output.
- State Data Center Outage – Any State Data Center mainframe or OS malfunction that does not allow the end user to access their system or send and receive information is to be considered as an unplanned outage for the State Data Center. The entire time that the system is unavailable is to be reported as State Data Center's system unavailable for that month.
- Customer Outage – If the customer's LAN goes down and the end user cannot access the system, the entire time that the LAN is down will not be considered as State Data Center's system unavailable for that month.

The State Data Center's service objective for system availability is 99% availability during normal hours of operation and 95% system availability during off-hours of operation. Since planned downtime is scheduled with advance notice to the customer, it is not counted against the system availability objective.

Service Support

The Service Support Table below lists the type of support and hours of availability that the State Data Center guarantees to the customer. The customer agrees to provide first level support as described in this table. Support outside the indicated hours can be arranged by special request at an additional cost.

SERVICE SUPPORT TABLE

SERVICE TYPE	RESPONSIBILITY	HOURS
First Level	Customer or customer help desk	7:00AM - 5:00PM, Monday-Friday, excluding holidays
Second Level	State Data Center Help Desk	5:30 AM – 10:00 PM, Monday-Friday, 7:00 AM – 12:00 PM, Saturday; Via pager initiated by calling (916) 739-7640, 24 hours a day; 7 days a week
Third Level	State Data Center Server Support, Large Systems, Database Support, Internet Support, and Network Support	7:00AM – 5:00PM, Monday – Friday, excluding holidays. Technical staff available off-shift as required.

APPENDIX D - REPORTING

Monthly Reports

The State Data Center provides availability and performance reports as indicated in the table below and are posted to the DTS Intranet web site for customer review. The information contained in the reports reflects the past 30 days as well as provides data from previous months for trend analysis. Other service reports can be generated as agreed upon between the Customer and State Data Center. For example, State Data Center currently provides the following:

- Peak hour resource utilization
- CICS online transaction volume and Response time reports (daily, by 15 minute intervals)
- TSO response time
- Batch job turnaround time

METRICS	CALCULATION OR INFORMATION TO BE PROVIDED
System Availability (Normal Hours) -- Guaranteed hours -- Unscheduled hours -- Actual hours -- Percentage Available	# of work days in month * 10 Actual downtime Guaranteed hours – Unscheduled hours Actual hours / Guaranteed hours * 100
System Availability (Off-Hours) -- Guaranteed hours -- Unscheduled hours -- Actual hours -- Percentage Available	# of work days in month * 14 + # of non-work days * 24 – preventative maintenance hours Actual downtime Guaranteed hours – Unscheduled hours Actual hours / Guaranteed hours * 100
Data & Operational Recovery	Detailed information regarding system/file recovery from backup
Outage Information -- Server Systems	Detailed information regarding Server system outages. Information includes: up and down times, hardware/software failure point, and resolution (This information is contained in help desk problem tickets)

Server Hosting Reports

The State Data Center provides monthly billing records to the customer's designated representative for review.

Outage Reports

The State Data Center provides outage reports detailing outages in the electrical power, air conditioning, or fire suppression systems in use in the State Data Center computer room. Outage reports are provided only when and if an outage to any of the aforementioned systems occurs.

Internet/Web Monthly Reports

Standard statistical reports are available for customers who subscribe to hosting services for the standard monthly fee. A one time fee and on-going monthly fee based on DTS Published Consulting Rate applies to Assigned Web Hosting. Customized reports are available and developed for the customer at an hourly Internet Design and Development rate. These reports are log file dependent, monthly fee pays for hardware, software, maintenance, internal support costs, and data center admin or overhead costs.

Standard statistical reports include the following:

- Resources accessed
- Site visitors and demographics
- Site activity statistics
- Technical statistics
- Site referrers & keywords
- Site visitors, browsers & operating systems platforms

Telecommunications Division Monthly Reports

The Telecommunications Division generates the Major Network Outage Report on a monthly basis, which reflects all of the outages that occurred during the month. This report describes the following:

- Date/time
- Remedy Ticket Number
- Description of Outage
- Number of Downed Sites
- Total Outage Time
- Customer Impact